GDAŃSK UNIVERSITY
OF TECHNOLOGY

Bezpieczeństwo systemu multimedialnych

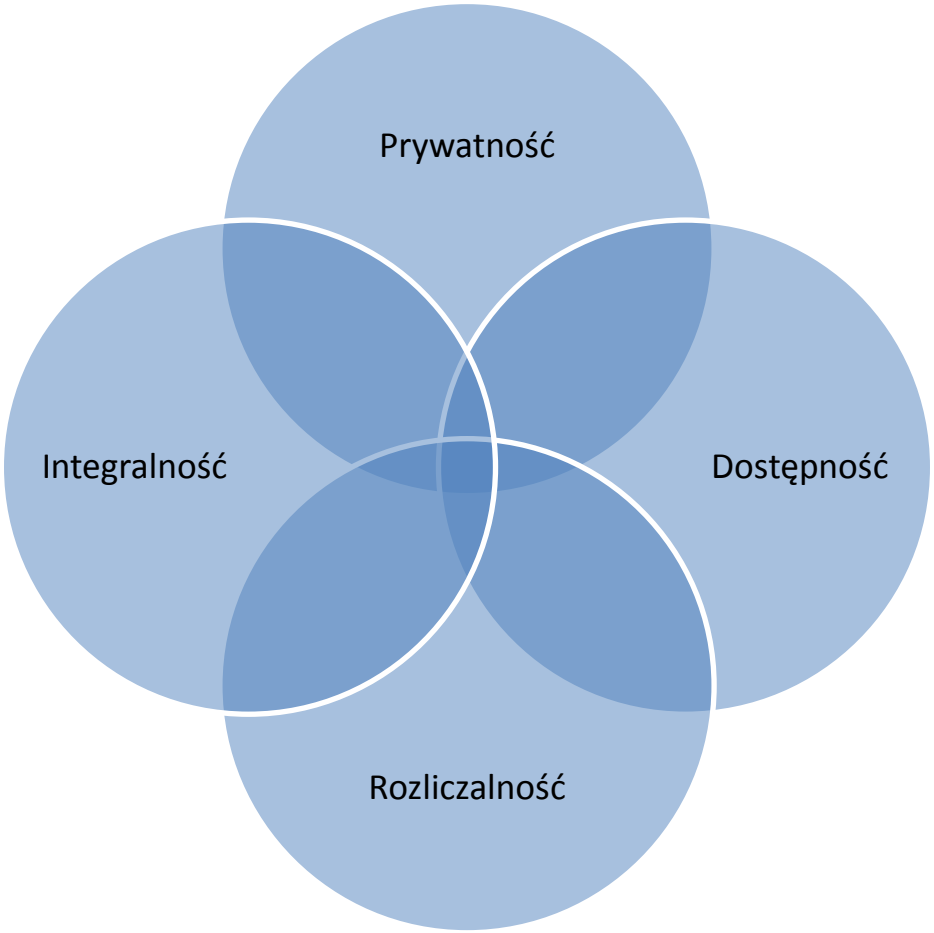
Michał Hoeft

GDAŃSK UNIVERSITY OF TECHNOLOGY

- Co zmienia się w bezpieczeństwie systemów multimedilanych w kontekście migracji do sieci IP?

GDAŃSK UNIVERSITY OF TECHNOLOGY

Grupy zagrożeń



- Zagrożenia dotyczące prywatności:
  - Możliwość przechwycenia strumieni multimedialnych
  - Możliwość rekonstrukcji strumieni multimedialnych
  - Analiza wzorców zachowań
  - Gromadzenie danych kontaktowych

GDAŃSK UNIVERSITY OF TECHNOLOGY

- Zagrożenia dotyczące integralności
  - Modyfikacja parametrów transmisji
  - Przekierowanie transmisji
  - Podszycie do uczestnika transmisji
  - Fałszowanie taryfikacji
  - Modyfikacja zawartości transmisji

- Zagrożenia dotyczące dostępności usługi
  - Masowe przesyłanie wiadomości (ataki DOS, DDoS)
  - Nieautoryzowane zakończenie połączenia
  - Zakłócenie mechanizmów zapewnienia QoS

- Zagrożenia związane z rozliczalnością usługi:
  - Możliwość wykonywania połączeń naliczanych innym użytkownikom
  - Możliwość wykonywania kosztownych połączeń obciążających właściciela systemu

GDAŃSK UNIVERSITY OF TECHNOLOGY

Wektory ataku

- Wspólne z współistniejącymi systemami
  - Zagrożenia OS
  - Ataki na sieć
- Specyficzne dla konkretnych rozwiązań
  - Błędy protokolarne
- Wspólne z współistniejącymi systemami ale wzmocnione przez specyfikę systemu
  - Socjotechnika
- Błędy w implementacji
- Bezpieczeństwo sieci IP
    - System VoIP jest tak bezpieczny jak sieć, w której pracuje

- Potencjalne ataki
  - SPIT (Spam over IP Telephony)
  - Podsłuchiwanie rozmów
  - DoS/DDoS/TDoS
  - Problem zmiany oprogramowania firmware
  - Fraudy
  - Wyciek danych w strumieniu RTP
  - Registration Hijacking

GDAŃSK UNIVERSITY OF TECHNOLOGY

WYBRANE METODY ZABEZPIECZENIA

GDAŃSK UNIVERSITY OF TECHNOLOGY

Metody zabezpieczenia

- Bezpieczeństwo sygnalizacji
  - Secure SIP (SIPS)
- Bezpieczeństwo transmisji danych
  - SRTP
  - IPSec ESP

GDAŃSK UNIVERSITY OF TECHNOLOGY

SIPS

- SIPS wprowadza mechanizmy analogiczne do HTTPS
  - SIP over TLS
  - Brak możliwości zastosowania UDP dla protokołu TLS
- Możliwość uwierzytelnienia serwera realizowana z wykorzystaniem certyfikatu
- Uwierzytelnienia klienta:
  - Username/digest
  - Możliwość wykorzystania certyfikatu

GDAŃSK UNIVERSITY OF TECHNOLOGY

SIPS

- Zabezpieczenie jedynie *hop-by-hop*
  - Możliwość odczytania wiadomości w każdym serwerze przetwarzającym komunikację
  - Przydatne do zabezpieczenia pierwszej mili
- Brak zabezpieczenia *end-to-end*

GDAŃSK UNIVERSITY OF TECHNOLOGY

SRTP – Secure RTP/RTCP

- Zdefiniowany dla transmisji typu unicast i multicast
- Dodatkowy narzut 4-14 bajtów (4B MKI, 4-10B authentication Tag)
- Zapewnienie poufności oraz integralności
  - Szyfrowanie domyślnie: AES-CM 128
  - Integralności: HMAC-SHA1

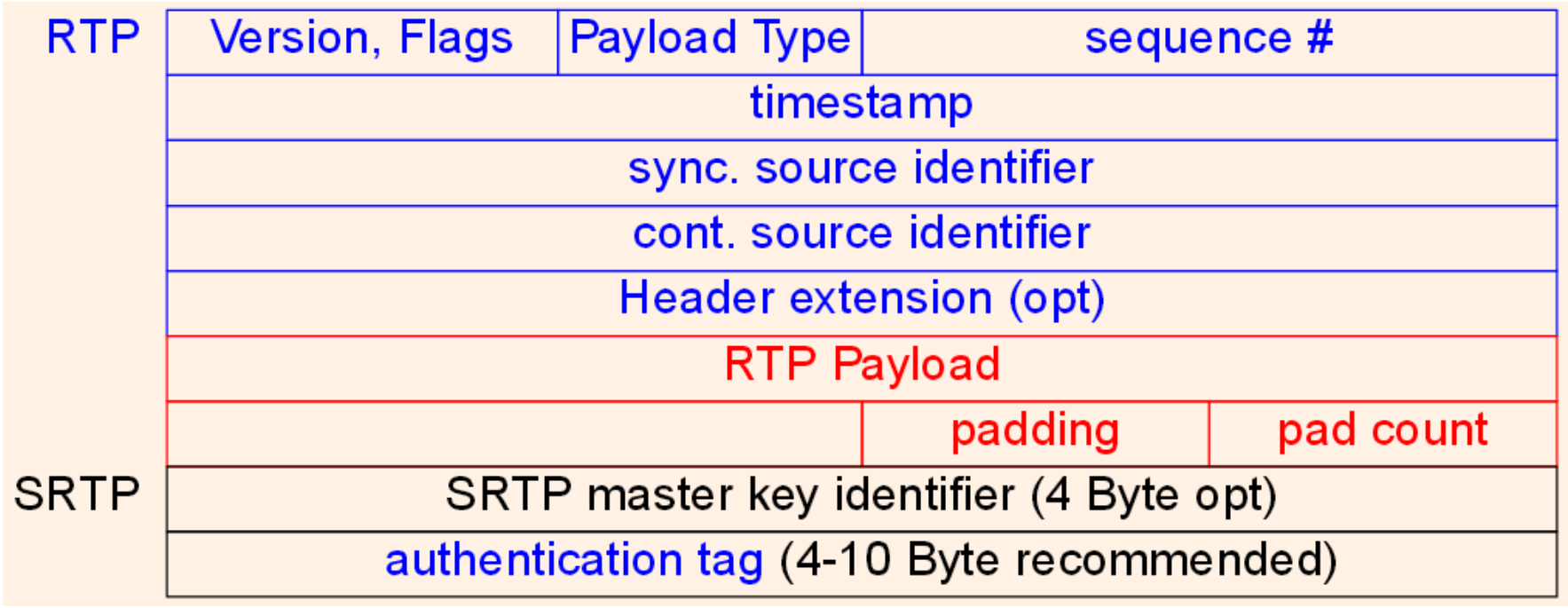
GDAŃSK UNIVERSITY OF TECHNOLOGY

SRTP – Secure RTP/RTCP

- Niezależny kanał zarządzania kluczami
  - Potrzebny tylko jeden klucz typu master
  - Poszczególne klucze dla SRTP generowane na podstawie klucza master:
    - Sesyjny klucz szyfrujący
    - Sesyjny klucz uwierzytelniający
  - Niezależne klucze dla SRTP oraz SRTCP

GDAŃSK UNIVERSITY OF TECHNOLOGY

SRTP – Secure RTP/RTCP



http://www.hznet.de/security/voipsec.pdf

GDAŃSK UNIVERSITY OF TECHNOLOGY

Dostarczanie klucza

- W wiadomości SDP

```
INVITE sip:642022@example.net SIP/2.0
Via: SIP/2.0/udp 1.25.43.66:5060;branch=z9hG4bK5E04B432A7CE4D494016D27E86B2D
From: <sip:hoz@sip.example.de>;tag=1167B5B5D227AA6656B12714F8441
To: <sip:642022@example.net>
Call-ID: 135F08716ED07E5D0C0B7B855BC21@1.25.43.66
CSeq: 9 INVITE
Contact: <sip:hoz@1.25.43.66;uniq=964E34A1883165EE1829BFAE36988>
Max-Forwards: 70
User-Agent: AVM FRITZ!Box Fon WLAN 7170 29.04.02 (Jan 25 2006)
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE, PRACK, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE
Content-Type: application/sdp
Accept: application/sdp, multipart/mixed
Content-Length:   381

v=0
o=user 10512055 10512055 IN IP4 1.25.43.66
s=call
c=IN IP4 1.25.43.66
t=1144829986 1144835586
k=base64:acx4fimF1pQdu6y2QTzttXjr5Z3eOVmmVu4YRZQoKqc=
m=audio 7078 RTP/AVP 8 0 3 102 100 97
a=sendrecv
a=rtpmap:2 G726-32/8000
a=rtpmap:102 G726-32/8000
a=rtpmap:100 G726-40/8000
a=rtpmap:97 iLBC/8000
a=fmtp:97 mode=30
a=rtcp:7079
```

http://www.hznet.de/security/voipsec.pdf

GDAŃSK UNIVERSITY OF TECHNOLOGY

Dostarczanie klucza

- W wiadomości SDP

```
INVITE sip:642022@example.net SIP/2.0
Via: SIP/2.0/udp 1.25.43.66:5060;branch=z9hG4bK5
From: <sip:hoz@sip.example.de>;tag=1167B5B5D227A
To: <sip:642022@example.net>
Call-ID: 135F08716ED07E5D0C0B7B855BC21@1.25.43.6
CSeq: 9 INVITE
Contact: <sip:hoz@1.25.43.66;uniq=964E34A1883165
Max-Forwards: 70
User-Agent: AVM FRITZ!Box Fon WLAN 7170 29.04.02
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE
Content-Type: application/sdp
Accept: application/sdp, multipart/mixed
Content-Length:   381

v=0
o=user 10512055 10512055 IN IP4 1.25.43.66
s=call
c=IN IP4 1.25.43.66
t=1144829986 1144835586
k=base64:acx4fimF1pQdu6y2QTzttXjr5Z3eOVmmVu4YRZQoKqc=
m=audio 7078 RTP/AVP 8 0 2 102 100 97
a=sendrecv
a=rtpmap:2 G726-32/8000
a=rtpmap:102 G726-32/8000
a=rtpmap:100 G726-40/8000
a=rtpmap:97 iLBC/8000
a=fmtp:97 mode=30
a=rtcp:7079
```

Istotne aby wiadomości SDP były dostarczane przez SIPS

http://www.hznet.de/security/voipsec.pdf

GDAŃSK UNIVERSITY OF TECHNOLOGY

VPN

- Wirtualne sieci prywatne
  - Podłączenie do sieci korporacyjnej użytkowników z sieci wizytowanych
  - Podłączenie sieci korporacyjnej do operatora (trunk)
  - Połączenie pomiędzy operatorami VoIP

GDAŃSK UNIVERSITY OF TECHNOLOGY

PRAKTYKA

GDAŃSK UNIVERSITY OF TECHNOLOGY

DoS/DDoS

- Scenariusz
  - Zalewanie urządzania niechcianym ruchem
    - SIP INVITE, SIP OPTIONS
    - RTP
    - Inne protokoły np. DNS, ICMP itp.
- Większość urządzeń nie posiada dużej mocy obliczeniowej
- Efekty
  - Spadek jakości
  - Niestabilna praca urządzenia

GDAŃSK UNIVERSITY OF TECHNOLOGY

Fuzzing

- Scenariusz
  - Przesyłane do urządzenia wiadomości zawierają błędne (pod względem składni protokołu) dane
- Możliwość niespodziewanego zachowania urządzenia

GDAŃSK UNIVERSITY OF TECHNOLOGY

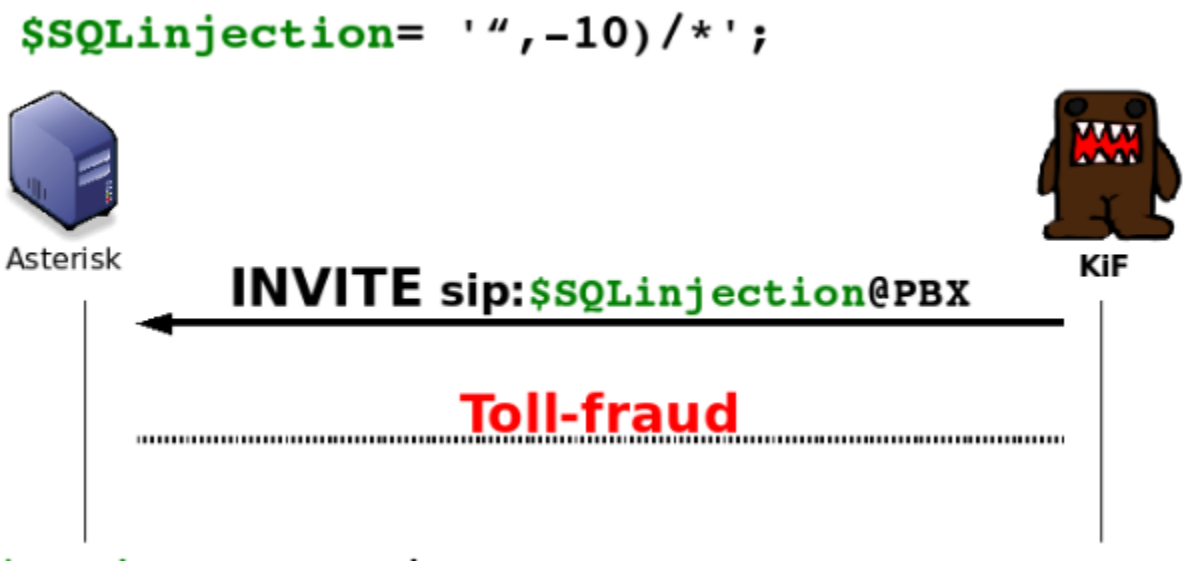
Manipulacja sygnalizacją

- Scenariusz
  - Przesyłane do urządzenia wiadomości zawierają poprawne pod względem składni dane, ale prowadzą do niespodziewanego zachowania urządzenia
- Różnorodny efekt zależny od realizowanego scenariusza

GDAŃSK UNIVERSITY OF TECHNOLOGY

Błędy w implementacji

- Ataki SQL injection



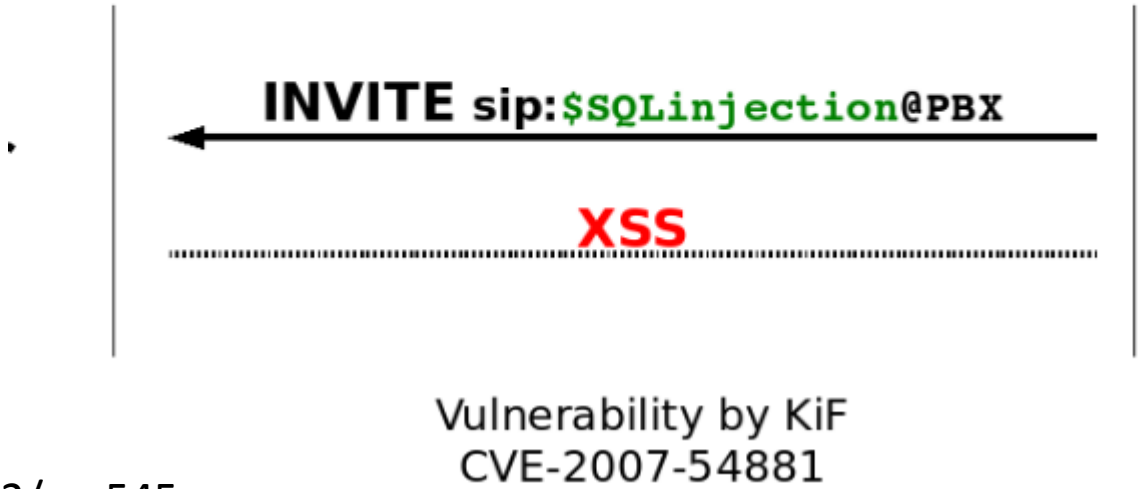
http://www.cse.psu.edu/~pdm12/cse545-s11/slides/cse545-voip.pdf

GDAŃSK UNIVERSITY OF TECHNOLOGY

- Ataki XSS

```
$script= '<script>
                alert("Hello world")
          </script>';

$SQLinjection= '"'.2hex($script).')/*';
```



Vulnerability by KiF
CVE-2007-54881

http://www.cse.psu.edu/~pdm12/cse545-s11/slides/cse545-voip.pdf

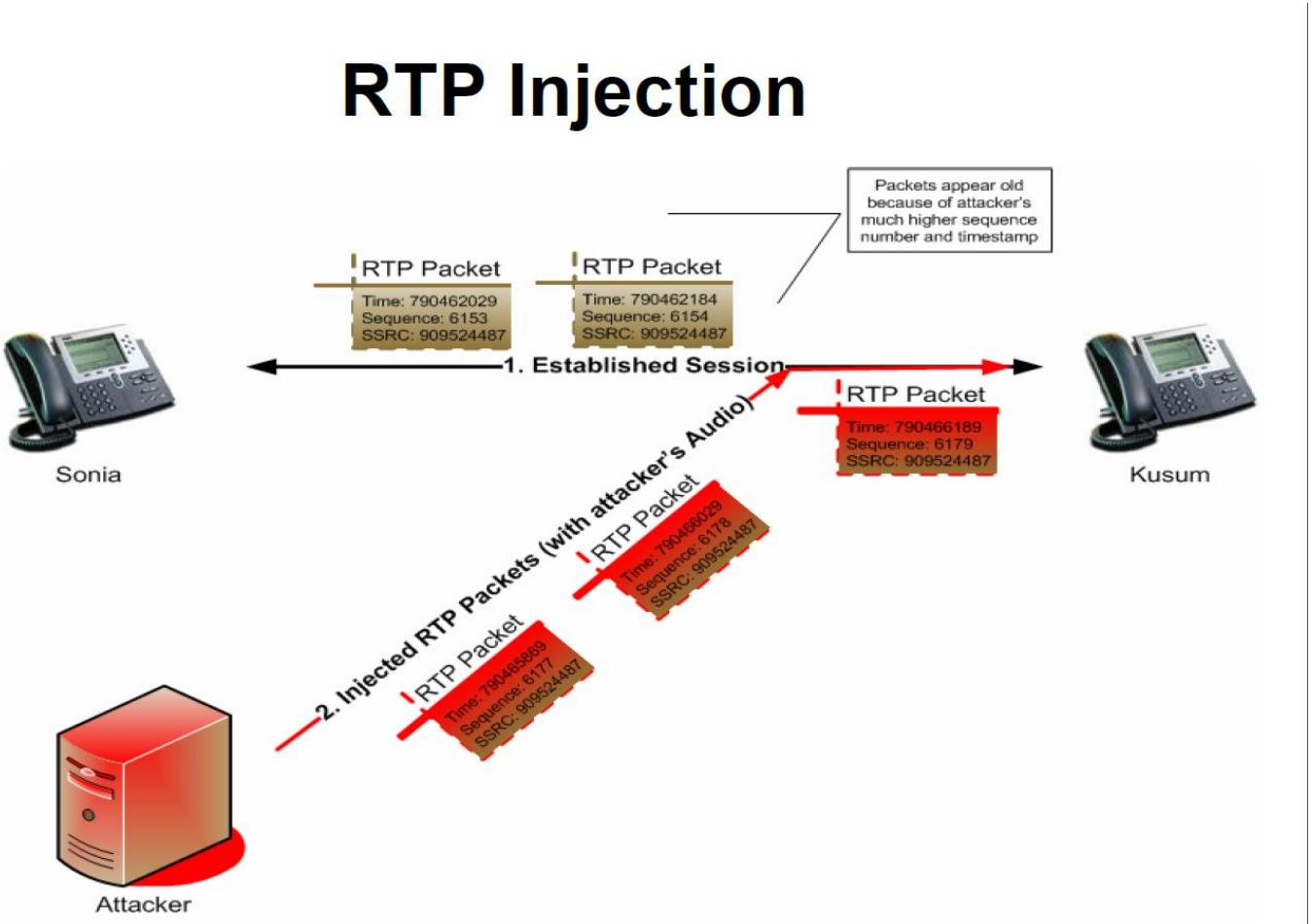
GDAŃSK UNIVERSITY OF TECHNOLOGY

Media Injection

- Scenariusz
  - Do odbiorcy dostarczane są niespodziewane pakiety RTP
    - W UDP łatwo wstrzyknąć ruch
    - Numery sekwencyjne i znaczniki czasu w RTP do przewidzenia
- Odbiorca otrzyma zmodyfikowany strumień audio

GDAŃSK UNIVERSITY OF TECHNOLOGY

Modyfikacja strumienia RTP



GDAŃSK UNIVERSITY OF TECHNOLOGY

Steganografia

- Scenariusz
  - Strumień RTP jest wykorzystywany do transmisji danych inne niż dane multimedialne
    - Potencjalnie stosunkowo duża przepływność
    - Stosunkowo długi czas połączenia
    - Trudność w wykryciu

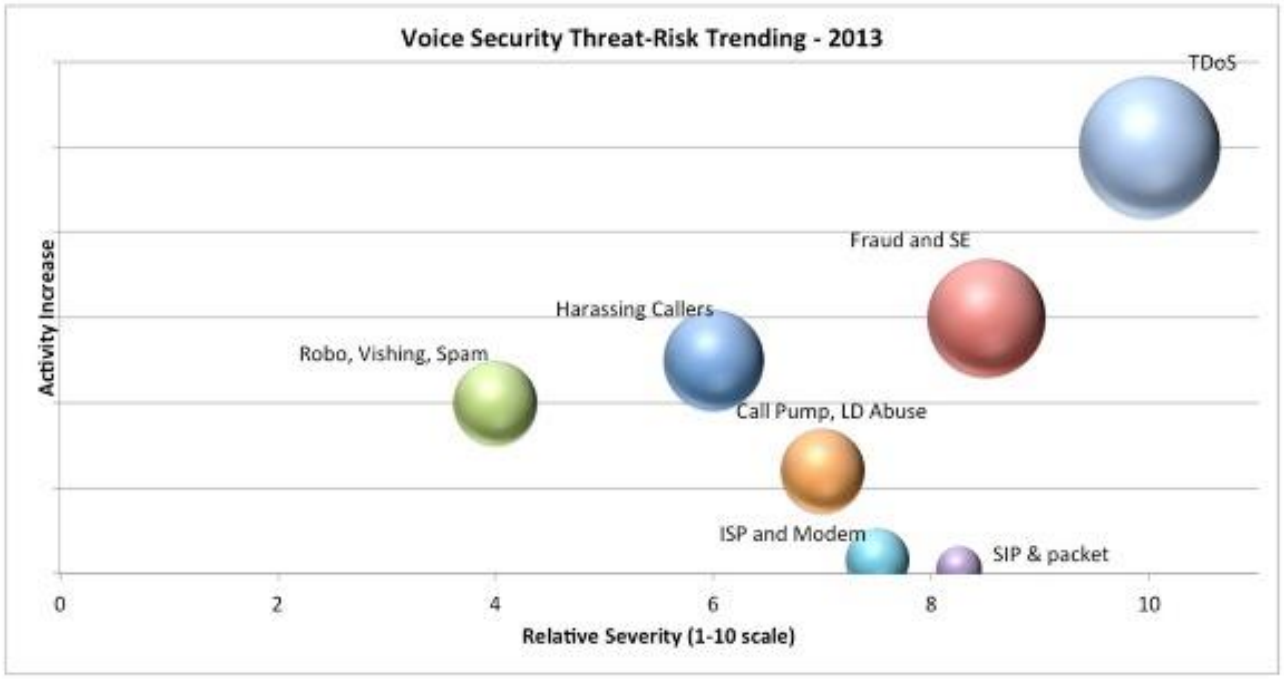
GDAŃSK UNIVERSITY OF TECHNOLOGY

Telephony Denial of Service

- Telephony Denial of Service – TDoS
  - Atak polegający na angażowaniu osób obsługujących połączenia VoIP
  - Prowadzi odmowy realizacji usługi wynikającej nie z braku zasobów technicznych a osób
  - Trudny do identyfikacji i wykrycia
    - Problem klasyfikacji wywołań

GDAŃSK UNIVERSITY OF TECHNOLOGY

UC Security Overview



iSight

SecureLogix

http://www.slideshare.net/isightsoftware/keeping-denial-of-service-and-financial-fraud-out-of-your-contact-center

GDAŃSK UNIVERSITY OF TECHNOLOGY

Metody TDoS

- Caller ID spoof Reflection Attack
- Malware
- Infected smart-phones
- Smart phones botnets

GDAŃSK UNIVERSITY OF TECHNOLOGY

Fraud

Phone Hackers Dial and Redial to Steal Billions

By NICOLE PERLROTH OCT. 19, 2014

Email
Share
Tweet
Save
More

SAN FRANCISCO — Bob Foreman's architecture firm ran up a $166,000 phone bill in a single weekend last March. But neither Mr. Foreman nor anyone else at his seven-person company was in the office at the time.

"I thought: 'This is crazy. It must be a mistake,' " Mr. Foreman said.

It wasn't. Hackers had broken into the phone network of the company, Foreman Seeley Fountain Architecture, and routed $166,000 worth of calls from the firm to premium-rate telephone numbers in Gambia, Somalia and the Maldives. It would have taken 34 years for the firm to run up those charges legitimately, based on its typical phone bill, according to a complaint it filed with the Federal Communications Commission.

Hackers targeted the phone system at Bob Foreman's architecture firm in Georgia, making $166,000 in calls in a weekend. Tami Chappell for The New York Times

Hackers targeted the phone system at Bob Foreman's architecture firm in Georgia, making $166,000 in calls in a weekend. Credit Tami Chappell for The New York Times

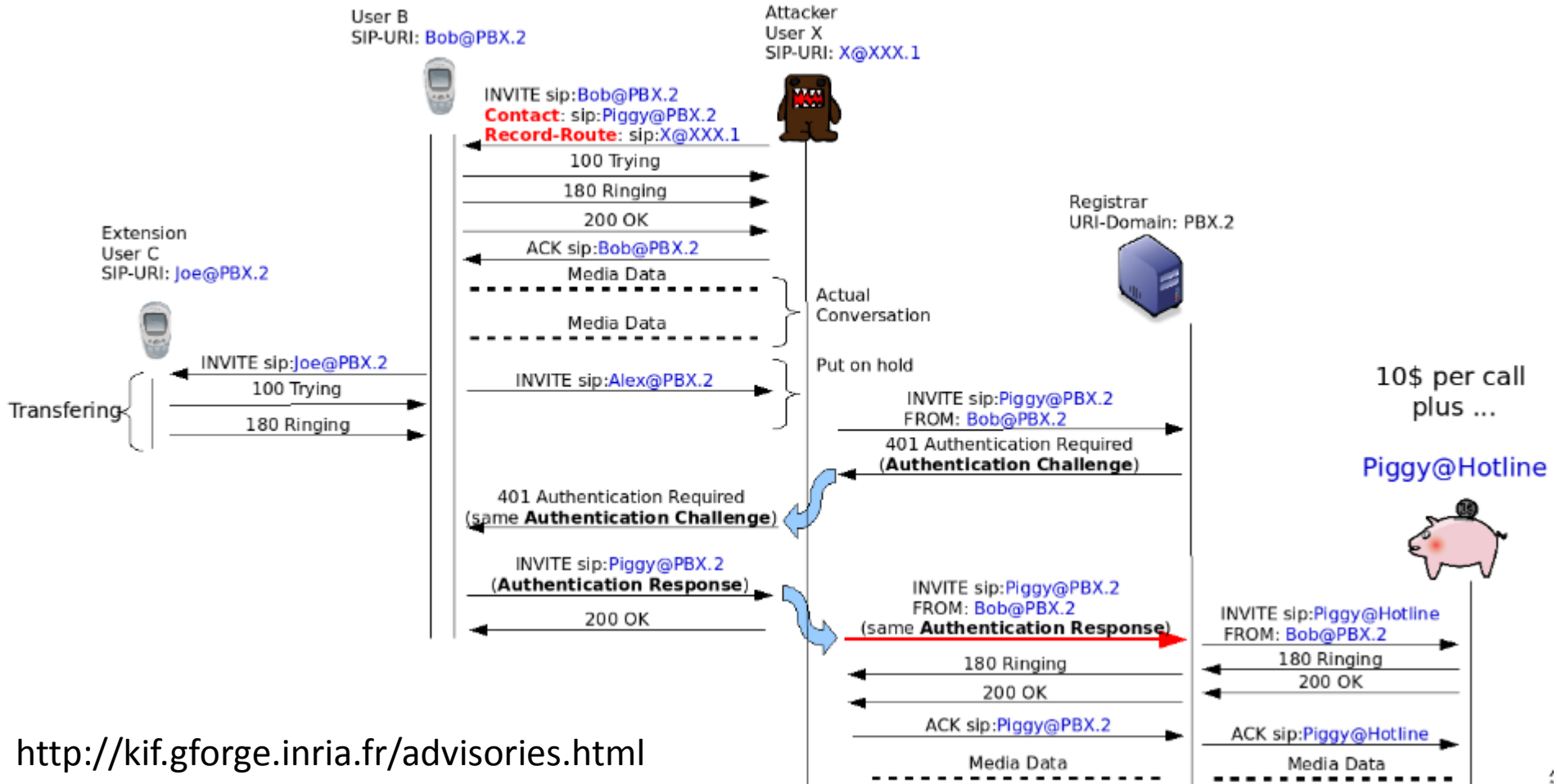
GDAŃSK UNIVERSITY OF TECHNOLOGY

Fraud

- Scenariusz
  - Nasz system zostaje skompromitowany pozwalając na nawiązywanie połączeń z kosztownymi odbiorcami
- Różne metody i wektory ataku

GDAŃSK UNIVERSITY OF TECHNOLOGY

SIP digest authentication relay attack



http://kif.gforge.inria.fr/advisories.html

GDAŃSK UNIVERSITY OF TECHNOLOGY

PODŁĄCZENIE PBX W SIECI

GDAŃSK UNIVERSITY OF TECHNOLOGY

- Jak podłączyć IP PBX do naszej sieci?

GDAŃSK UNIVERSITY OF TECHNOLOGY

PROBLEM TRANSLACJI ADRESÓW

GDAŃSK UNIVERSITY OF TECHNOLOGY

NAT

- NAT
  - Pozwala zrealizować odwzorowanie dużej liczby adresów prywatnych na mniejszą liczbę adresów publicznych
  - Zapewnia „ukrycie” wewnętrznej topologii
  - Czy jest to mechanizm bezpieczeństwa?

GDAŃSK UNIVERSITY OF TECHNOLOGY

NAT

- NAT
  - Pozwala zrealizować odwzorowanie dużej liczby adresów prywatnych na mniejszą liczbę adresów publicznych
  - Zapewnia „ukrycie” wewnętrznej topologii
  - Czy jest to mechanizm bezpieczeństwa?
  - Połączenie może być zrealizowane z sieci lokalnej ale nie do niej

GDAŃSK UNIVERSITY OF TECHNOLOGY

NAT

- Problemy z translacją NAT w systemach VoIP
  1. Protokoły sygnalizacyjne przenoszą informację o danych adresowych (SDP) generowane po stronie klienta. Adres i numer portu ulegają zmianie przy zastosowaniu NAT
  2. Klient musi pierwszy wysłać pakiet należący do strumienia aby „otworzyć” port na urządzeniu NAT

GDAŃSK UNIVERSITY OF TECHNOLOGY

NAT

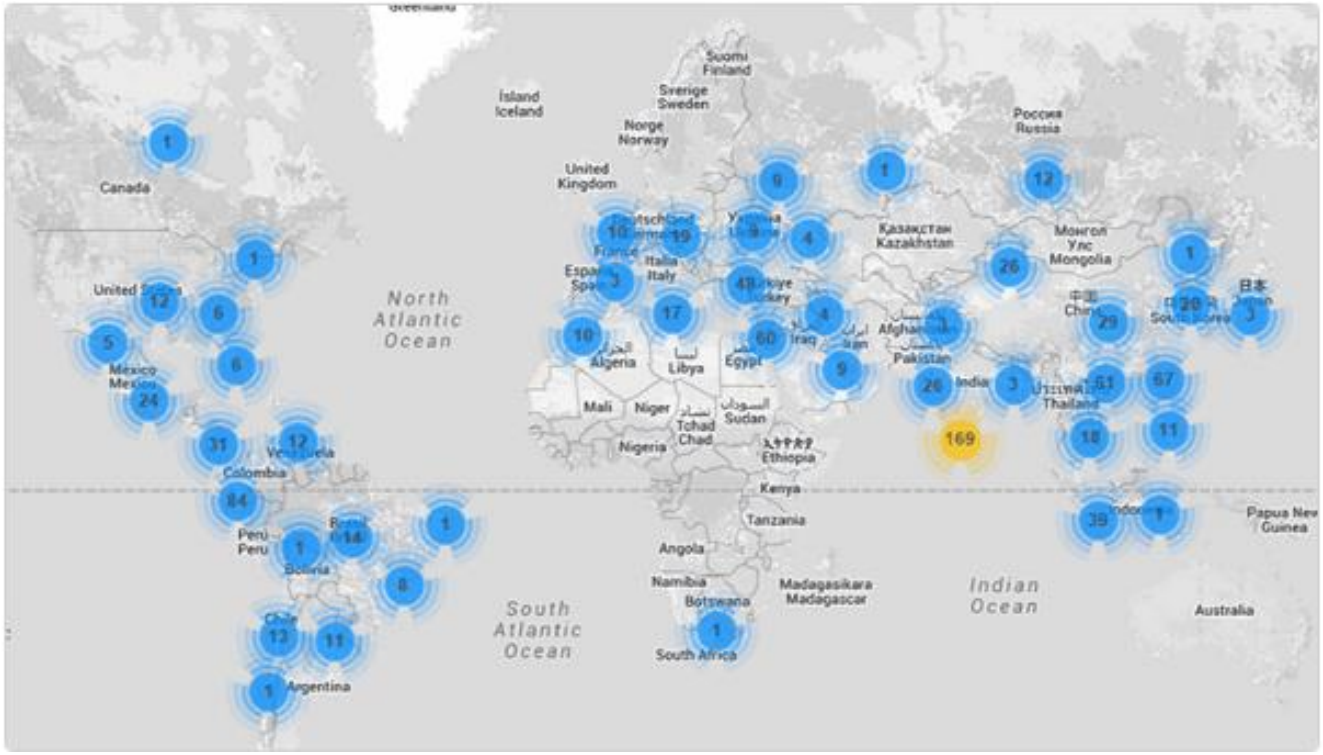
- Rozwiązania 1.
  - Protokół IPv6
  - UPnP
  - SIP extensions for NAT (RFC 5381)
  - STUN (Simple Traversal of UDP Through NAT)
  - TURN (Traversal Using Relay NAT)
  - ICE (Interactive Connectivity Establishment)
  - SIP ALG zintegrowany z NAT

GDAŃSK UNIVERSITY OF TECHNOLOGY

NASZ SYSTEM MOŻE BYĆ ZAGROŻENIEM !

GDAŃSK UNIVERSITY OF TECHNOLOGY

- **CCTV DDoS Botnet**
  - **900 urządzeń z całego świata**



https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

Ostatnie 2 największe ataki DDoS

- **OVH:**
  „This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.”
- **Brian Krebs:**
  - ~620 Gbps
- Niemal dowolny ruch z całego świata, bez potrzeby użycia amplifikacji

GDAŃSK UNIVERSITY OF TECHNOLOGY

DZIĘKUJĘ ZA UWAGĘ